Amendments to the Drawings:

The attached sheets of drawings include changes to Figures 1 and 2. These sheets, which include Figures 1 and 2, replace the original sheets including Figures 1 and 2.

Attachment: Replacement Sheets

REMARKS

Claims 1-21 are presented for further examination. Claims 1, 3, 11-13, 15, 16, and 18-20 have been amended.

In the Office Action mailed September 29, 2008, the Examiner required a drawing under 37 C.F.R. § 1.81(c). In addition, claims 1-21 were rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent Publication No. 2002/0066014 ("Dworkin"). Applicants respectfully disagree with the basis for the rejection and request reconsideration and further examination of the claims.

Drawings

Applicants are unclear as to whether there is an objection to the drawings or if formal drawings are requested. Applicants are submitting herewith substitute formal drawings and respectfully request that the drawings be approved and entered in the application. No new matter has been added.

Claim Rejection

Claim 1, as amended, is directed to an apparatus arranged to accept digital data as an input and to process the data according to one of either a Secure Hash Algorithm (SHA-1) or Message Digest (MD5) algorithm to produce a fixed length output word. The apparatus is recited as including a plurality of rotational registers coupled to a read bus to receive and store data, one of the registers arranged to receive the input data.

Claim 1 further recites data stores coupled to the read bus for initialization of some of the plurality of registers according to the algorithm selected to be used, the data stores including fixed data relating to the selected operation. A plurality of dedicated combinatorial logic circuits are also recited having inputs coupled to the read bus and outputs coupled to the write bus and arranged to perform logic operations on data stored in selected ones of the plurality of registers and to output to the write bus. Claim 1 concludes with a plurality of temporary data storage registers having inputs coupled to the write bus and outputs coupled to the read bus, an

output of one of the temporary data storage registers comprising an output of the apparatus for the fixed length output work.

In summary, the apparatus of claim 1 utilizes the data from the rotational registers that is placed on the read bus through operations using the combinatorial logic circuits, the output of which is sent to the write bus. The data stores for initialization of the plurality of registers are coupled to the read bus to initialize at least selected ones of the rotational registers. The output from the combinatorial logic circuits is received at the input of the temporary data storage registers. The output of the plurality of temporary data storage registers can be sent to the read bus for further operations by the combinatorial logic circuits, or the output of the one temporary data storage register for the circuit can be used as the output of the circuit for the fixed length output word.

Dworkin, U.S. Patent Publication No. 2002/0066014, teaches a completely different circuit that has the disadvantages discussed in the background of the present application, *i.e.*, a greater number of processor clock cycles to complete the operations, substantially more topographical area for the circuit, and greater power consumption.

More particularly, Dworkin utilizes register files 12 to hold intermediate and final results of its operations, some of which can be preset to specific values according to an algorithm and which can contain chaining variables. The output of these registers is sent to a function circuit 22 that includes logic functions, the output data values of which are received at a summing and adder circuit 30. A word wise circular queue 32 has data words stored in registers for step and dependent words. Text messages to be operated upon are stored in register array 32 and output to the summing and adding circuit 30 to be combined with the data values output from the function circuit 22.

Depending on the operation to be performed, constants stored in additional registers 34 and 36 are input to the summing and adder circuit. The output of the summing and adding circuit 30 is then sent to either a barrel shifter 40 for further operations or thence to the register file 12 to be cycled back through the function and adder circuit 30 in accordance with the type of operation chosen.

Dworkin states that in the SHA-1 mode there are four rounds of processing, each round having twenty steps and in the MD5 mode there are four rounds of processing but each round has sixteen steps. In each of these rounds of processing and steps, "the output of function circuit 22 is connected to a summing circuit or adder 30" (see paragraph 0012).

Dworkin describes the altering of values stored in the registers to occur "on every clock cycle to contain chaining variables" (paragraph 0011), and admits that the computation of hash values "involves many clock cycles, with intermediate results stored as chaining variables" (paragraph 0010). This is precisely the type of computational overhead the present claimed embodiments seek to avoid as described in the background portion of the application.

More particularly, Dworkin sends the output from the input register, the register array, the function circuit, and the constants registers all to the summing and adder circuit 30. There is no summing and adder circuit in the present claimed embodiment. The arrangement of the claimed rotational registers and temporary data storage registers with the read and write busses eliminates the need for such an adder circuit. As a result, operations are quicker and overhead is reduced. Nowhere does Dworkin teach or suggest the use of a write bus and a read bus coupled to the registers in the manner recited in claim 1. Applicants respectfully submit that the combination recited in claim 1 is clearly not anticipated by Dworkin.

Dependent claims 2-10 are allowable for the features recited therein as well as for the reasons why claim 1 is allowable.

Independent claim 11 is directed to a circuit that includes a plurality of data storage registers coupled to a read bus to receive and store data; a plurality of shift registers for temporary data storage and having inputs coupled to a write bus and outputs coupled to the read bus, an output of one of the shift registers comprising an output of the circuit; a plurality of logic circuits having inputs coupled to the read bus and outputs coupled to the write bus for performing operations on data and to output to the write bus; and a control circuit configured to control the foregoing to selectively perform MD5 and SHA-1 operations on data.

As discussed above, nowhere does Dworkin teach or suggest the combination recited in claim 1 in which the data storage registers are coupled to a read bus, the shift registers for temporary data storage having inputs coupled to the write bus and outputs coupled to the read

bus, and logic circuits having inputs coupled to the write bus and outputs coupled to the read bus, and a control circuit for selectively performing the operations. Rather, Dworkin specifically teaches the use of a summing and adder circuit instead of the read and write busses of the present claimed embodiment. Applicants respectfully submit that claim 11 is clearly allowable over Dworkin, as are dependent claims 12-14.

Independent claims 15 and 19 are likewise directed to a circuit that includes the read and write busses as previously described that is not taught by Dworkin. Applicants respectfully submit these independent claims and their respective dependent claims are allowable for the reasons discussed above with respect to claims 1 and 11.

In view of the foregoing, applicants respectfully submit that all of the claims in this application are clearly in condition for allowance. In the event the Examiner disagrees or finds minor informalities that can be resolved by telephone conference, the Examiner is urged to contact applicants' undersigned representative by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

The Director is authorized to charge any additional fees due by way of this Amendment, or credit any overpayment, to our Deposit Account No. 19-1090.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:alb

Enclosure:
Two Sheets of Replacement Drawings (Figures 1-2)

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031

851663.479USPC / 1307707_1.DOC